A New Multi-Moduli Residue Number Systems with moduli of forms $2^{n_1}+1$, $2^{n_2}-1$, 2^{n_3}

The interested reader can find more information on the above subject in the following references:

References

[1]. M. Abdallah and A. Skavantzos, "A systematic approach for selecting practical moduli sets for residue number systems", in Proc. of the 27th IEEE Southeastern Symposium on System Theory, March 1995, pp. 445-449.

[2]. M. Abdallah and A. Skavantzos, "New Multi-Moduli Residue and Quadratic Residue Systems for Large Dynamic Ranges", in Proceedings of the Twenty-Ninth Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, Oct. 1995, pp. 961-965.

Theory

Consider the following sets

$$S_1 = \{ 2^1+1,\ 2^3+1,\ 2^5+1,\ 2^7+1,\ 2^9+1,\ \cdots\cdots,\ \}$$
$$S_2 = \{ 2^2+1,\ 2^6+1,\ 2^{10}+1,\ 2^{14}+1,\ 2^{18}+1,\ \cdots\cdots,\ \}$$
$$S_3 = \{ 2^4+1,\ 2^{12}+1,\ 2^{20}+1,\ 2^{28}+1,\ 2^{36}+1,\ \cdots\cdots,\ \} \quad (1)$$
$$S_4 = \{ 2^8+1,\ 2^{24}+1,\ 2^{40}+1,\ 2^{56}+1,\ 2^{72}+1,\ \cdots\cdots,\ \}$$
$$S_5 = \{ 2^{16}+1,\ 2^{48}+1,\ 2^{80}+1,\ 2^{112}+1,\ 2^{144}+1,\ \cdots\cdots,\ \}$$

where in general

$$S_d = \{ \text{all numbers } N_{k,d} \text{ such that } N_{k,d} = 2^{2^d k + 2^{d-1}} + 1 \ ; \quad (2)$$
$$k = 0, 1, 2, 3, \cdots\cdots, \}, \text{ where } d = 1, 2, 3, \cdots\cdots.$$

Observation: All the numbers in the S_d sets, $(d = 1, 2, 3, \cdots\cdots,)$, represent all possible integers of the form 2^n+1 for any $n = 1, 2, 3, \cdots\cdots$.

The binary exponents (i.e; the exponents of two) of the numbers of the S_d sets have the following properties.

Property 1: Exponents of adjacent numbers in any set S_d, $(d = 1, 2, 3, \cdots\cdots,)$, differ by 2^d.

Property 2: The number 2^n+1 belongs to the set S_d if and only if $\langle n \rangle_{2^d} = 2^{d-1}$.

In other words, what properties 1,2 dictate are:

- Property 1 dictates that exponents of adjacent numbers in sets $S_1, S_2, S_3, S_4, S_5, \ldots$ differ by $2, 4, 8, 16, 32, \ldots$, etc....
- Property 2 dictates that the binary exponents (ie; the exponents of two) for numbers belonging to sets $S_1, S_2, S_3, S_4, S_5, \ldots$, are of forms $2k+1, 4k+2, 8k+4, 16k+8, 32k+16, \ldots$, etc...

Lemma 1: The first number in any S_d set is a common divisor of all the numbers in the same set; (it divides all the numbers in the same set).

Theorem 1: Any two numbers of the form 2^n+1 are relatively prime if and only if they belong to two different S_d sets.

Theorem 2: If n_1 is any integer and n_2 is an odd integer, then the numbers $2^{n_1}+1$ and $2^{n_2}-1$ are relatively prime.

Theorem 3: The numbers $2^{n_1}-1$ and $2^{n_2}-1$ are relatively prime if and only if n_1 and n_2 are relatively prime.

- **Moduli Selection Rules**

The presented theorems provide the necessary background for selecting moduli sets with moduli of the forms $2^{n_1}+1$, $2^{n_2}-1$, 2^{n_3}. Some selection rules follow which can act as guidelines for such successful moduli selections.

1. Only one modulus of the form 2^s can be chosen.
2. Any number of moduli of the form 2^n+1 can be chosen, as long as they belong to different S_d sets (see Theorem 1). Together with these, the numbers $2^{n_1}-1, 2^{n_2}-1, \ldots, 2^{n_L}-1$ can be chosen as long as $n_1, n_2, \ldots, n_L$ are pairwise relatively prime odd integers (see Theorems 2, 3).
3. Only one modulus of the form 2^n-1 where n is even can be chosen (see Theorem 3). In this case, the number 2^n-1 must be factorized and its factors will then determine which numbers must be excluded from possible moduli choices.

For example, suppose that the number $2^{44}-1$ is chosen as one of the moduli choices. Observe that $2^{44}-1 = (2^{11}-1)(2^{11}+1)(2^{22}+1)$. Since $2^{11}+1 \in S_1$ and $2^{22}+1 \in S_2$, no numbers can be chosen from the sets S_1 and S_2; (see Theorem 1). Also, the number $2^{11}-1$ dictates that no number of the form 2^d-1 where $(d,11) \neq 1$ can be chosen (see Theorem 3).

4. The product of the moduli should be large enough in order to implement the desired dynamic range.

5. For a given dynamic range, the largest modulus should be as small as possible so that the RNS system can have the highest possible performance. This implies that the moduli m_i must be as close as possible to one another, creating this way a balanced decomposition of the dynamic range.

A new balanced 8-moduli set resulting from the presented theory follows:

- A new balanced 8-moduli set

$$P = \{m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8\}$$

$$= \{2^{n-3}-1,\ 2^{n-2}+1,\ 2^{n-1}-1,\ 2^{n}+1,\ 2^{n+1}-1,\ 2^{n+1}+1,$$
$$2^{n+2}+1,\ 2^{n+2}\}. \qquad (3).$$

where $n = 4k+2$, k is an integer.

The moduli of set P are pairwise relatively prime.

- The moduli m_6 and m_4 belong to sets S_1 and S_2 respectively (see property 2).
- Neither m_2 nor m_7 can belong to S_2 or S_1 (see property 2), while they have to belong to two different sets S_d and $S_{d'}$ where $d>2$, $d'>2$ and $d \neq d'$ (see property 1).

Therefore, m_2, m_4, m_6, m_7 belong to four diffent S_d sets and due to

Theorem 1 are pairwise relatively prime.

- The pairwise relatively prime exponents $n-3$, $n-1$, $n+1$ dictate that m_1, m_3, m_5 are also relatively prime in pairs (see theorem 3); (given the fact that $n-3$, $n-1$, $n+1$ are odd integers, can you prove that they are pairwise relatively prime??).
- Finally, theorem 2 suggests that the entire set P of eq. (3) consists of pairwise relatively prime moduli.

The set P is the most balanced 8-moduli set consisting of attractive moduli forms 2^a-1, 2^b+1, 2^c; (see that exponents of adjacent moduli differ by <u>at most</u> 1 (one)).

Example 1: Consider the previously presented 8-moduli set (the set P of (3)) for $n = 10$; (see that $10 = 4 \times 2 + 2$).
Then

$$P_{(n=10)} \equiv \{2^7-1, 2^8+1, 2^9-1, 2^{10}+1, 2^{11}-1, 2^{11}+1, 2^{12}+1, 2^{12}\}.$$

The dynamic range for such a system is

$$DR \cong (7+8+9+10+11+11+12+12) \text{ bits} = 80 \text{ bits}.$$

(B) The Quadratic Residue Number System (QRNS)

• Complex Multiplication in the ring Z_m

Consider two complex numbers $a+jb$ and $c+jd$ where $j=\sqrt{-1}$, $a\in Z_m$, $b\in Z_m$, $c\in Z_m$, $d\in Z_m$.

Then the product of the two complex numbers in Z_m is

$$\langle (a+jb)(c+jd) \rangle_m =$$

$$= \langle \langle ac \rangle_m - \langle bd \rangle_m \rangle_m + j \langle \langle ad \rangle_m + \langle bc \rangle_m \rangle_m$$

The computational requirement for the complex multiplication is four real multiplications and two additions.

• The Quadratic Residue Number System (QRNS)

The QRNS can perform the multiplication of two complex numbers using only two real multiplications. This achievement is possible if the quadratic equation $x^2+1=0$ has two distinct roots in Z_m.

- The QRNS mapping and inverse mapping

Consider a complex number $a+jb$ with $a \in Z_m$, $b \in Z_m$ and let r be a root of $x^2+1=0$ in Z_m; (this means that r is an integer such that $r \in Z_m$ and $\langle r^2+1 \rangle_m = 0$).

The QRNS mapping is described by

$$a+jb \xrightarrow{QRNS} (a^*, b^*) \qquad (4)$$

where

$$a^* = \langle a+rb \rangle_m \quad ; \quad b^* = \langle a-rb \rangle_m \qquad (5)$$

The inverse QRNS mapping is given by

$$(a^*, b^*) \xrightarrow{QRNS^{-1}} a+jb$$

where

$$a = \langle 2^{-1}(a^*+b^*) \rangle_m \qquad (6)$$

$$b = \langle 2^{-1} r (b^*-a^*) \rangle_m \qquad (7)$$

- Processing in the QRNS domain

Let $a, b, c, d \in Z_m$ and let the complex numbers $a+jb$ and $c+jd$ have the following QRNS representations:

$$a+jb \xrightarrow{QRNS} (a^*, b^*)$$
$$c+jd \xrightarrow{QRNS} (c^*, d^*)$$

Then

$$\langle (a+jb) \odot (c+jd) \rangle_m \xrightarrow{QRNS} (\langle a^* \odot c^* \rangle_m , \langle b^* \odot d^* \rangle_m)$$

where $\odot$ can be $+, -, \times$.

- Theorem 4: Let m be an integer and let its prime decomposition be $m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_L^{e_L}$, where $p_1, p_2, \cdots, p_L$ are prime integers while $e_1, e_2, \cdots, e_L$ are integers. Then the quadratic equation $x^2+1=0$ has two distinct roots in Z_m if and only if $p_i = 4k_i+1$, $i = 1, 2, \cdots, L$ where $k_1, k_2, \cdots, k_L$ are integers.

• Example 2: Using the QRNS technique perform in Z_{13} the complex multiplication $e+jf = \langle (a+jb)(c+jd) \rangle_{13}$ where $a=5$, $b=6$, $c=7$, $d=8$.

Solution: Here $m=13$ is a prime and $13 = 4\times 3+1$. The QRNS Theorem[4] then dictates that $x^2+1=0$ has two distinct roots in Z_{13}. One such root is $r=5$ (observe that $\langle 5^2+1 \rangle_{13} = \langle 26 \rangle_{13} = 0$).

• QRNS Mapping:

The QRNS mapping described by eqs (4) – (5) gives

$$a+jb = 5+j6 \xrightarrow{QRNS} (a^*, b^*) = (\langle 5+5\times 6 \rangle_{13}, \langle 5-5\times 6 \rangle_{13})$$
$$= (9, 1).$$

$$c+jd = 7+j8 \xrightarrow{QRNS} (c^*, d^*) = (\langle 7+5\times 8 \rangle_{13}, \langle 7-5\times 8 \rangle_{13})$$
$$= (8, 6).$$

• QRNS Multiplication:

$$e+jf = \langle (a+jb)(c+jd) \rangle_m \xrightarrow{QRNS} (\langle a^* c^* \rangle_m, \langle b^* d^* \rangle_m)$$
$$= (\langle 9\times 8 \rangle_{13}, \langle 1\times 6 \rangle_{13}) = (7, 6) = (e^*, f^*).$$

- **QRNS Inverse Mapping:**

Equations (6), (7) give

$$(e^*, f^*) \xrightarrow{QRNS^{-1}} (e, f)$$

where

$$e = \langle 2^{-1}(e^* + f^*) \rangle_m = \langle 2^{-1}(7+6) \rangle_{13} = 0$$

$$f = \langle 2^{-1} \cdot r (f^* - e^*) \rangle_m = \langle 7 \times 5 \times (6-7) \rangle_{13} = 4$$

Thus $e + jf = \langle (a+jb)(c+jd) \rangle_{13} = 0 + j4.$

- **Double check:**

$$\langle (5+j6)(7+j8) \rangle_{13} = \langle 5\times7 - 6\times8 \rangle_{13} + j \langle 5\times8 + 6\times7 \rangle_{13}$$

$$= \langle -13 \rangle_{13} + j \langle 82 \rangle_{13} = 0 + j\,4.$$

B-1 Multi-Moduli QRNS Systems with Coprime Moduli

One can design multi-moduli QRNS systems based on moduli sets

$$R = \{m_1, m_2, \ldots, m_L\}$$

The mathematical requirement is that the moduli $m_1, m_2, \ldots, m_L$ must be pairwise relatively prime and also in agreement with theorem 4.

Due to the fact that hardware simplicity is achieved when using the attractive moduli forms $2^{n_1}+1$, $2^{n_2}-1$, 2^{n_3}, only these forms will be considered here. Unfortunatelly, only forms 2^n+1 with n being even are allowed. Forms $2^{n_1}+1$ with n_1 being odd, as well as forms $2^{n_2}-1$ and 2^{n_3} are not appropriate for QRNS. Theorem 4 dictates that for a modulus m to be appropriate for QRNS, each of its

prime factors must be of form $4k+1$. Therefore, m must also be of form $4k+1$. However, neither 2^{n_3}, nor $2^{n_2}-1$ can be of form $4k+1$. Regarding numbers $2^{n_1}+1$ will n_1 being odd, they all get divided by 3 (see lemma 1) while the prime # 3 is not of form $4k+1$.

Consider a complex number $a+jb$ with $a \in Z_m$, $b \in Z_m$ and $m = 2^n+1$ with n being an even integer. Then $r = 2^{\frac{n}{2}}$ is a root of $x^2+1=0$ in Z_{2^n+1}; (observe that

$$r^2 < \left(2^{\frac{n}{2}}\right)^2 + 1 >_{2^n+1} = < 2^n+1 >_{2^n+1} = 0).$$

The QRNS mapping is then described by

$$a+jb \xrightarrow{QRNS} (a^*, b^*)$$

where

$$a^* = < a + 2^{\frac{n}{2}} \cdot b >_{2^n+1} \; ; \quad b^* = < a - 2^{\frac{n}{2}} \cdot b >_{2^n+1} \qquad (8)$$

The inverse QRNS mapping is given by

$$(a^*, b^*) \xrightarrow{QRNS^{-1}} a+jb$$

where

$$a = \left\langle -2^{n-1}(a^* + b^*) \right\rangle_{2^n+1} \qquad (9)$$

$$b = \left\langle 2^{\frac{n}{2}-1}(b^* - a^*) \right\rangle_{2^n+1} \qquad (10)$$

Equations (8) – (10) dictate that if $m = 2^n + 1$ (n even), the QRNS mapping and inverse mapping rely on additions and multiplications by powers of 2. Such multiplications by powers of 2 require rotations and complement operations if diminished-1 representations of numbers are used.

- Moduli Selection

Since the only allowed attractive forms are $2^n + 1$ (n even), any number of moduli of this form can be chosen as long as they belong to different S_d sets with $d \neq 2$; (see S_d sets of (1), (2) and theorem 1). of course, adjacent moduli must be

as close as possible to one another so that the QRNS system is balanced.

A balanced 3-moduli QRNS set is

$$A=\{m_1, m_2, m_3\}=\{2^{n-2}+1,\ 2^{n}+1,\ 2^{n+2}+1\} \quad (11)$$

where $n=4k+2$, $k=1,2,3,\ldots$

Here $m_2 \in S_2$ while m_1 and m_3 belong to two different sets S_d and $S_{d'}$ where $d>2$, $d'>2$ and $d\neq d'$; (see explanations following set P of equation (3)). Also, set A is the most balanced 3-moduli set as the binary exponents of adjacent moduli differ by two; (the exponents are even).

Set A can be expanded into set B

$$B=\{m^*, m_1, m_2, m_3\}$$
$$=\{2^{n-6}+1,\ 2^{n-2}+1,\ 2^{n}+1,\ 2^{n+2}+1\} \quad (12)$$

where $n=8k+6$, $k=1,2,3,\ldots$

Again, $m_2 \in S_2$ while m_1 and m_3 belong to two different sets S_d and $S_{d'}$ where $d>2$, $d'>2$, $d \neq d'$. The restriction $n=8k+6$ ensures that $2^{n-6}+1$ and $2^{n+2}+1$ do not belong to set S_3. Therefore, the four moduli of set B belong to four different S_d sets and according to theorem 1 they are pairwise relatively prime.

Adding one or two more moduli to set B, one gets the sets C and D

$$C=\{2^{n-14}+1,\ 2^{n-6}+1,\ 2^{n-2}+1,\ 2^{n}+1,\ 2^{n+2}+1\} \quad (13)$$

where $n=16k+14$, $k=1,2,3,\ldots$

$$D=\{2^{n-30}+1,\ 2^{n-14}+1,\ 2^{n-6}+1,\ 2^{n-2}+1,\ 2^{n}+1,\ 2^{n+2}+1\} \quad (14)$$

where $n=32k+30$, $k=1,2,3,\ldots$.

Let DR_A, DR_B, DR_C, DR_D be the dynamic ranges achieved by sets A, B, C, D. Then

$$\left\{\begin{array}{l} DR_A = 3n \text{ bits}. \\ DR_B = 4n-6 \text{ bits}. \\ DR_C = 5n-20 \text{ bits}. \\ DR_D = 6n-50 \text{ bits}. \end{array}\right\}$$

A comparison between sets A, B, C, D results in the following observations:

1. Sets A, B, C, D are the most balanced 3-, 4-, 5-, 6-moduli QRNS sets with relatively prime moduli of forms 2^n+1.
2. All sets imply the same speed performance (largest modulus is $2^{n+2}+1$).
3. Regarding their dynamic ranges, $DR_B > DR_A$ for $n>6$, $DR_C > DR_B$ for $n>14$, $DR_D > DR_C$ for $n>30$.
4. The differences in the binary exponents between the largest and the smallest moduli for sets A, B, C, D are 4, 8, 16, and 32 respectively. Thus, sets A and B imply more balanced QRNS arithmetic than sets C and D.
5. The choices of n are more restricted for sets C and D when compared to the choices of n for sets A and B.

- The Big Problem:

From the above observations, it is clear that for QRNS sets with more than four moduli of form 2^n+1 (n even), selecting pairwise relatively prime moduli creates problems. This is due to the fact that as the number of moduli increases, the selection process becomes less flexible; (i.e., severe restrictions are placed on the choices of n). For example, set D is defined for $n = 62, 94, 126, \ldots$. These values of n are very restricted and they also force the dynamic ranges to be unrealistically large implying impractical QRNS systems. In addition, sets with five or more moduli result in very unbalanced QRNS arithmetic.

- Question: Is there any solution for the above mentioned problem??
- Answer: YES
- Question: So what is the solution?
- Answer: Go to next page ⟶ →

B-2 Multi-Moduli QRNS Systems with Noncoprime Moduli of forms 2^n+1

Here a solution to the above mentioned problem is offered by considering QRNS systems with noncoprime moduli of forms 2^n+1. The interested reader can find more information on this subject in the following reference:

References

[3]. M. Abdallah and A. Skavantzos, "On the binary quadratic residue system with noncoprime moduli", IEEE Transactions on Signal Processing, vol. 45, no. 8, pp. 2085-2091, August 1997.

A theorem follows which provides the mathematical basis for the current subject.

Theorem 5: Consider two numbers

$N_{d,k} = 2^{2^{d-1}(2k+1)} + 1$ and $N_{d,k'} = 2^{2^{d-1}(2k'+1)} + 1$

belonging to the same S_d set (see S_d sets of eqs. (1), (2)). Let

$N_{d,0} = 2^{2^{d-1}} + 1$ be the first number in set S_d. Then the numbers $\frac{N_{d,k}}{N_{d,0}}$ and $\frac{N_{d,k'}}{N_{d,0}}$ are relatively prime if and only if $2k+1$ and $2k'+1$ are relatively prime.

Example 3: Consider the numbers $2^{10}+1$, $2^{14}+1$, $2^{18}+1$, $2^{22}+1$, $2^{26}+1$. All these five numbers belong to the set S_2. Their binary exponents are 10, 14, 18, 22, 26. The odd parts of these exponents are 5, 7, 9, 11, 13. These five numbers

5, 7, 9, 11, 13 are pairwise relatively prime. Therefore, according to theorem 5, the numbers $\frac{2^{10}+1}{2^2+1}$, $\frac{2^{14}+1}{2^2+1}$, $\frac{2^{18}+1}{2^2+1}$, $\frac{2^{22}+1}{2^2+1}$, $\frac{2^{26}+1}{2^2+1}$ are also pairwise relatively prime.

Theorems 1 and 5 dictate that multimoduli QRNS sets can be constructed using moduli from different S_d sets as well as from the same S_d set; $(d \geq 2)$.

The design methodology for constructing multimoduli QRNS systems is described by the following steps:

1. Moduli of the form $m_i = 2^{n_i}+1$ (n_i even) are chosen from the same S_d set as well as from different S_d sets $(d \geq 2)$. The moduli chosen from the same S_d set must be in agreement with Theorem 5 in the sense that the add parts of their exponents should be pairwise relatively prime.

Of course, adjacent moduli must be as close as possible to one another so that the QRNS system is balanced.

2. All weighted to RNS conversions, QRNS mappings, QRNS processing, and inverse QRNS mappings are performed using set

$$Q = \{m_1, m_2, \cdots, m_L\} \quad (15)$$

where $m_i = 2^{n_i} + 1$ (n_i even). Set Q consists of nonrelatively prime moduli and since all of them are of the attractive form $2^n + 1$, the above mentioned transactions rely on simple hardware.

3. The RNS to weighted conversion is performed using set

$$Q' = \{m_1', m_2', \cdots, m_L'\} = \left\{\frac{m_1}{c_1}, \cdots, \frac{m_L}{c_L}\right\} \quad (16)$$

Set Q' consists of pairwise relatively prime integers, the product of which defines the actual dynamic range of the QRNS system.

The scale-down factors c_i are dictated by theorem 5. Each c_i is either 1 or the first number of some S_d set. The Chinese Remainder Theorem (CRT) reconstruction for converting the RNS vector $(Z_1, Z_2, \cdots, Z_L)$ into its weighted form using set Q' is shown by

$$Z = \left\langle \sum_{i=1}^{L} \langle Z_i N_i' \rangle_{m_i'} M_i' \right\rangle_{M'} \qquad (17)$$

where

$$m_i' = \frac{m_i}{c_i}, \quad M' = \prod_{i=1}^{L} m_i', \quad M_i' = \frac{M'}{m_i'},$$

$$N_i' = \langle (M_i')^{-1} \rangle_{m_i'} \; ; \; i = 1, 2, \cdots, L.$$

Some new QRNS sets with noncoprime moduli of forms 2^n+1 (n even) are now presented. A new four-moduli set is

$$A_1 = \{m_0, m_1, m_2, m_3\} = \{2^{n-4}+1, 2^{n-2}+1, 2^n+1, 2^{n+2}+1\} \; ; \; n = 4k+2 \; ; \; k = 2, 3, 4, \cdots, \qquad (18)$$

Set A_1 is an expansion of set A of (11) in the sense that it includes the extra modulus $m_0 = 2^{n-4}+1$. The restriction $n = 4k+2$ implies that $m_0, m_2 \in S_2$ (see property 2). Therefore, m_0, m_2 are not relatively prime (see theorem 1). The binary exponents of m_0, m_2 are $n-4 = 4k-2$, $n = 4k+2$ while the odd parts of these exponents are $\frac{n-4}{2} = 2k-1$ and $\frac{n}{2} = 2k+1$ which are relatively prime. Therefore $m_0' = \frac{m_0}{2^2+1} = \frac{m_0}{5}$ and $m_2' = \frac{m_2}{2^2+1} = \frac{m_2}{5}$ are also relatively prime; (see theorem 5). The set A_1 is the most balanced four-moduli QRNS set since the even binary exponents of adjacent moduli differ by two. The actual dynamic range achieved by set A_1 of (18) is defined by $\frac{m_0}{5} \times m_1 \times \frac{m_2}{5} \times m_3 \cong 2^{4n-9}$ or

$$DR_{A_1} = 4n-9 \text{ bits} \qquad (19).$$

Adding one more modulus to set A_1 of (18) yields set A_2

$$A_2=\{2^{n-8}+1,\ 2^{n-4}+1,\ 2^{n-2}+1,\ 2^{n}+1,\ 2^{n+2}+1\} \quad (20)$$

where $n=4k+2$, $k=3,4,5,\cdots$.

Here, $2^{n-8}+1$, $2^{n-4}+1$, $2^{n}+1$ belong to set S_2, while $\frac{n-8}{2}=2k-3$, $\frac{n-4}{2}=2k-1$, $\frac{n}{2}=2k+1$ are relatively prime in pairs. Theorem 5 then dictates that $\frac{2^{n-8}+1}{5}$, $\frac{2^{n-4}+1}{5}$, $\frac{2^{n}+1}{5}$ are also pairwise relatively prime. The actual dynamic range achieved by set A_2 is

$$DR_{A_2}=5n-19 \text{ bits} \quad (21).$$

Expanding set B of (12) by one or two more moduli yields sets B_1, B_2 where

$$B_1=\{2^{n-6}+1,\ 2^{n-4}+1,\ 2^{n-2}+1,\ 2^{n}+1,\ 2^{n+2}+1\} \quad (22)$$

$$B_2=\{2^{n-8}+1,\ 2^{n-6}+1,\ 2^{n-4}+1,\ 2^{n-2}+1,\ 2^{n}+1,\ 2^{n+2}+1\} \quad (23)$$

where $n=8k+6$, $k=1,2,3,\cdots$, ... for both B_1, B_2.

The noncoprime moduli in each of the sets B_1 and B_2 belong to set S_2. Also, sets B_1, B_2 are the most balanced 5-moduli and 6-moduli QRNS

sets with moduli of forms 2^n+1 (the even binary exponents of adjacent moduli differ by <u>two</u> in both sets B_1 and B_2). The actual dynamic ranges achieved by sets B_1, B_2 are

$$DR_{B_1} = 5n-15 \text{ bits} \qquad (24).$$

$$DR_{B_2} = 6n-25 \text{ bits} \qquad (25).$$

To see the benefits obtained by using multimoduli QRNS sets with noncoprime moduli of forms 2^n+1 (n even) consider comparing the moduli sets C, A_2, B_1 of equations (13), (20), (22). The following hold true:

1. The above three sets are 5-moduli sets.
2. These three sets imply the same speed performance (largest modulus is $2^{n+2}+1$).
3. The set C (which contains coor coprime moduli) achieves smaller dynamic range as compared to the ranges achieved by the noncoprime moduli sets A_2, B_1.

Just see that $DR_C = 5n - 20$ bits, $DR_{A_2} = 5n - 19$ bits, $DR_{B_1} = 5n - 15$ bits

4. Set C is the most unbalanced when compared to sets A_2 and B_1. Just see that the differences in the binary exponents between the largest and the smallest moduli for sets C, A_2, B_1 are 16, 10, 8.

5. The choices of n are much more restricted for set C when compared to the choices of n for sets A_2, B_1. See that set C is defined for $n = 30, 46, 62, 78, 94, \cdots$; Set A_2 is defined for $n = 14, 18, 22, 26, 30, 34, \cdots$; set B_1 is defined for $n = 14, 22, 30, 38, 46, \cdots$

The advantages obtained by using multi-moduli QRNS sets with noncoprime moduli are even more obvious when comparing the 6-moduli sets D (which contains

coprime moduli) and B_2 (which consists of noncoprime moduli). Both sets D and B_2 imply the same speed-performance (largest modulus is $2^{n+2}+1$) and therefore the comparison is fair. Set B_2 enjoys a dynamic range that is 2^{25} times larger than the dynamic range achieved by set D; (see that $DR_D = 6n-50$ bits; $DR_{B_2} = 6n-25$ bits). Set D is very unbalanced (largest exponent − smallest exponent = 32) while set B_2 is the most balanced 6-moduli QRNS set with moduli of forms 2^n+1; (the even binary exponents of adjacent moduli differ by <u>two</u>). Finally, the choices of n are <u>much</u> more restricted for set D when compared to choices of n for set B_2. See that set D is defined for $n = 62, 94, 126, 158, 190, \ldots$ while set B_2 is defined for $n = 14, 22, 30, 38, 46, \ldots$.

• Some More Good News:

The good news so far is that by using the new theory (the S_d sets of (1), (2) and theorems 1 and 5) it was possible to construct multi-

moduli QRNS systems based on sets with noncoprime moduli of attractive forms 2^n+1. The benefits obtained were very large dynamic ranges, very balanced arithmetic, flexible moduli choices, and still preserving the attractive moduli forms $m=2^n+1$ for the internal processing.

Question: Is this the end of the good news??

Answer: BUT OF COURSE NOT!!!

Question: So, what is the next good news?

Answer: The next good news is that by using the newly developed theory (the S_d sets of C1), C2) and the Theorems 1, 2, 3, 5) it has been possible to construct multi-moduli RNS (not QRNS) systems based on sets with noncoprime moduli pairs of the very attractive form $2^{ni}-1$, $2^{ni}+1$.

This new class of multimoduli RNS systems

is based on sets of form

$$P = \{ m_1, m_1^*, m_2, m_2^*, \cdots, m_L, m_L^* \} =$$

$$= \{ 2^{n_1}-1, 2^{n_1}+1, 2^{n_2}-1, 2^{n_2}+1, \cdots, 2^{n_L}-1, 2^{n_L}+1 \} \quad (26)$$

where the exponents $n_1, n_2, \cdots, n_L$ must be as close as possible to one another so that RNS arithmetic is as balanced as possible.

Definition 1: The numbers $m_i = 2^{n_i}-1$ and $m_i^* = 2^{n_i}+1$ are called conjugates of each other.

The new RNS systems which rely on pairs of conjugate moduli result in hardware-efficient 2-level implementations for the weighted-to-RNS and RNS-to-weighted conversions, achieve very large dynamic ranges and imply fast and efficient RNS internal processing. when compared to conventional systems of the same number of moduli and the

Same dynamic range, the new systems offer the following benefits: 1). Hardware savings of 25% to 40% for the weighted-to-RNS conversion. 2). A reduction of over 80% to 90% in the complexity of the final Chinese Remainder Theorem (CRT) involved in the RNS-to-weighted conversion. Thus, significant compromises between large dynamic ranges, fast internal processing and low complexity are achieved by these new systems.

• The interested reader can find more information on this subject in the following references:

References

[4]. A. Skavantzos and M. Abdallah, "Novel Residue Arithmetic Processors for High Speed Digital Signal Processing", in Proceedings of the Thirty Second Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, November 1998, pp. 187–193.

[5]. A. Skavantzos and M. Abdallah, "Implementation issues of the two-level residue number system with pairs of conjugate moduli", IEEE Transactions on Signal Processing, vol. 47, no. 3, pp. 826–838, March 1999.

Error Detection and Error Correction in Residue Number Systems.

In this handout, the subject of error detection and error correction in Residue Number Systems is studied.

Consider an RNS system based on moduli $m_1, m_2, \cdots, m_L$ where the moduli are pairwise relatively prime integers. To achieve error detection/error correction, some <u>redundant</u> moduli must be added to the system. Let the redundant moduli be $m_{L+1}, m_{L+2}, \cdots, m_{L+r}$. Such a system is then called Redundant Residue Number System (RRNS). For such a system, all the $L+r$ moduli $m_1, m_2, \cdots, m_L, m_{L+1}, \cdots, m_{L+r}$ are pairwise relatively prime. Some definitions follow:

- The moduli $m_1, m_2, \cdots, m_L$ are called <u>non redundant moduli.</u>
- The moduli $m_{L+1}, m_{L+2}, \cdots, m_{L+r}$ are called <u>redundant moduli.</u>

- The dynamic range achieved by the non redundant moduli is called <u>legitimate dynamic range</u>. This is to say that

> Legitimate dynamic range = $[0 \quad M-1]$
> where $M = m_1 \times m_2 \times \cdots \times m_L$

- The total dynamic range is

> Total dynamic range = $[0 \quad M_T - 1]$
> where $M_T = m_1 \times m_2 \times \cdots \times m_{L+r}$

- The illegitimate range is:

> Illegitimate range = $[M \quad M_T - 1]$

Let a number X have the following RRNS representation:

$$X \xrightarrow{\text{RRNS}} (X_1, X_2, \cdots, X_L, X_{L+1}, \cdots, X_{L+r})$$

where $X_i = \langle X \rangle_{m_i}$, $i = 1, 2, \cdots, L+r$.

The elements X_i are the residues or <u>residue digits</u> of X.

By error detection/error correction in RNS systems we mean techniques by which residue digits in error (faulty residue digits) can be detected, located and corrected. The following theorem is in place:

Theorem 1: A Redundant Residue Number System (RRNS) with r redundant moduli will allow detection of r residue digits in error or correction of $\lfloor \frac{r}{2} \rfloor$ residue digits in error [1]-[2]. Here, $\lfloor\ \rfloor$ denotes the floor function.

An obvious implication of theorem 1 is that to be able to correct a single residue digit in error, the number of redundant moduli must be r=2; (see that $\lfloor \frac{2}{2} \rfloor = 1$).

Error detection and correction of a single residue digit in error.

Consider a Redundant Residue Number System (RRNS) with L non redundant moduli and r=2 redundant moduli. Let the non redundant moduli be $m_1, \cdots, m_L$ while the redundant ones are m_{L+1}, m_{L+2}. Here, the L+2 moduli $m_1, \cdots, m_L, m_{L+1}, m_{L+2}$ are pairwise relatively prime integers. Also, each redundant modulus is larger than each non redundant modulus. Let a number X have the following residue-digit representation in this RRNS:

$$X \xrightarrow{\text{RRNS}} (X_1, \cdots, X_L, X_{L+1}, X_{L+2})$$

where $X_i = \langle X \rangle_{m_i}$, $i = 1, 2, \cdots, L, L+1, L+2$.

Assume the following:

(i). Assume that the number X belongs to the legitimate range. This means that overflow of the legitimate range has not occured. This can easily be accomplished by overflow prevention schemes.

(ii). Assume that at most one residue digit can be in error; (no more than one X_i can be in error, where $i = 1, \cdots, L+2$).

(iii). Assume that the hardware for converting the RNS into the weighted system is error free; (it functions correctly).

• The procedure for error detection/error correction of a single residue digit being in error is as follows:

1. Using the moduli set $\{m_1, m_2, \cdots, m_L, m_{L+1}, m_{L+2}\}$, convert the residue representation $(X_1, X_2, \cdots, X_L, X_{L+1}, X_{L+2})$ into its weighted form X. The Chinese Remainder Theorem (CRT) or the Mixed Radix Conversion (MRC) can be used for this conversion. If the obtained number X belongs to the illegitimate range, then an error has occured. otherwise, no error occured.

2. To locate and correct a residue digit in error, (if an error occured), compute the m_i – projections of X, $i = 1, 2, \cdots, L, L+1, L+2$. Let the m_i – projection of X be denoted as X_i^*. It is a well known fact that in case of a single residue digit being in error, one and only one projection will belong to the legitimate range, while all the other projections will belong to the illegitimate range [3], [2]. If X_i^* (the m_i – projection of X) belongs to the legitimate range, then the error occured in the i^{th} residue digit. In this case, the correct value of X is X_i^* and the correct residue digit X_i is $X_i = \langle X_i^* \rangle_{m_i}$.

- Question: what is the definition of X_i^* = The m_i – projection of X ?
- Answer:

X_i^* = The m_i – projection of X =

= Result of converting the residue representation $(X_1, X_2, \cdots, X_{i-1}, X_{i+1}, \cdots, X_{L+2})$ into a weighted number using the moduli set $\{m_1, m_2, \cdots, m_{i-1}, m_{i+1}, \cdots, m_{L+2}\}$. The CRT or MRC can be used for such conversions.

*** NOTE: As seen, in computing X_i^*, all the residue-digits except X_i participate. Also, all the moduli except m_i are used.

Example 1: This example will demonstrate the procedure for detecting, locating and correcting a single residue digit becoming faulty.

Consider a Redundant RNS (RRNS) based on set

$$S = \{m_1, m_2, m_3, m_4, m_5\} =$$

$$= \{5, 6, 7, 11, 13\}$$

(8) j

Here, the non redundant moduli are m_1, m_2, m_3 while the redundant moduli are m_4 and m_5.

The legitimate, total and illegitimate ranges are:

Legitimate range = $[0 \quad (5\times6\times7)-1] = [0 \quad 209]$.

Total range = $[0 \quad (5\times6\times7\times11\times13)-1] = [0 \quad 30,029]$

Illegitimate range = $[210 \quad 30,029]$.

Consider performing (using the above RRNS) the computation $Z = X + Y$, where $X = 128$ and $Y = 69$. As seen, the expected result $Z = X + Y = 128 + 69 = 197$ belongs to the legitimate range; (overflow of the legitimate range has not occured).

Converting X and Y into the above RRNS yields:

(9) j

$$X \xrightarrow{RRNS} (X_1, X_2, X_3, X_4, X_5) =$$

$$= (\langle 128 \rangle_5, \langle 128 \rangle_6, \langle 128 \rangle_7, \langle 128 \rangle_{11}, \langle 128 \rangle_{13})$$

$$= (3, 2, 2, 7, 11).$$

$$Y \xrightarrow{RRNS} (Y_1, Y_2, Y_3, Y_4, Y_5) =$$

$$= (\langle 69 \rangle_5, \langle 69 \rangle_6, \langle 69 \rangle_7, \langle 69 \rangle_{11}, \langle 69 \rangle_{13})$$

$$= (4, 3, 6, 3, 4).$$

Then

$$Z = X + Y \xrightarrow{RRNS} (Z_1, Z_2, Z_3, Z_4, Z_5) =$$

$$= (\langle 3+4 \rangle_5, \langle 2+3 \rangle_6, \langle 2+6 \rangle_7, \langle 7+3 \rangle_{11},$$

$$\langle 11+4 \rangle_{13} = (2, 5, 5, 10, 2)$$

or

$$Z \xrightarrow{RRNS} (Z_1, Z_2, Z_3, Z_4, Z_5) = (2, 5, 5, 10, 2)$$

What happened ??

Let's now see if the residue representation $(Z_1, Z_2, Z_3, Z_4, Z_5) = (2, 5, 5, 10, 2)$ is error-free or not.

Using the moduli set $\{m_1, m_2, m_3, m_4, m_5\} = \{5, 6, 7, 11, 13\}$, we convert the residue representation $(Z_1, Z_2, Z_3, Z_4, Z_5) = (2, 5, 5, 10, 2)$ into its weighted form Z. The computations yielding Z are shown in the Appendix at the end of this handout; (the CRT is used). The obtained result of this conversion is $Z = 13,067$. Since $Z = 13,067$ belongs to the illegitimate range, an error has occured; (this is error detection).

To now locate and correct the error, the m_i – projections of Z must be computed; $(i = 1, 2, 3, 4, 5)$. These projections are denoted by $Z_1^*, Z_2^*, Z_3^*, Z_4^*, Z_5^*$. The computations of these projections are also shown in the appendix and the CRT is used again.

As a reminder, the projection Z_1^* is the result of converting (Z_2, Z_3, Z_4, Z_5) into its weighted form using set $\{m_2, m_3, m_4, m_5\}$, the projection Z_2^* is the result of converting (Z_1, Z_3, Z_4, Z_5) into its weighted form using set $\{m_1, m_3, m_4, m_5\}$ etc...

These projections are found to be:

$Z_1^* = 1,055$; (Z_1^* belongs to illegitimate range).

$Z_2^* = 3,057$; (Z_2^* belongs to illegitimate range).

→ $Z_3^* = 197$; (Z_3^* belongs to legitimate range)

$Z_4^* = 2,147$; (Z_4^* belongs to illegitimate range).

$Z_5^* = 1,517$; (Z_5^* belongs to illegitimate range).

Since Z_3^* belongs to the legitimate range, (all the remaining projections belong to the illegitimate range), the error occured in the residue digit Z_3. In this case the correct value of Z is $Z = Z_3^* = 197$ and the correct residue-digit Z_3 is $Z_3 = \langle Z_3^* \rangle_{m_3} = \langle 197 \rangle_7 = 1$ or $\boxed{Z_3 = 1}$.

Problem: Consider a Redundant RNS (RRNS) based on moduli set

$$S = \{m_1, m_2, m_3, m_4\} = \{3, 4, 5, 7\}.$$

Here, the non redundant moduli are m_1, m_2 while the redundant moduli are m_3, m_4. Let a number X have the following residue-digit representation in this RRNS:

$$X \xrightarrow{\text{RRNS}} (X_1, X_2, X_3, X_4) = (1, 2, 3, 3)$$

where of course $X_i = \langle X \rangle_{m_i}$, $i = 1, 2, 3, 4$.

(13) j

Let the conversion of (X_1, X_2, X_3, X_4) into the weighted system using set $\{m_1, m_2, m_3, m_4\}$ yields the number $X = 178$.

Let the m_i – projections of X be $X_1^* = 38$, $X_2^* = 73$, $X_3^* = 10$ and $X_4^* = 58$, respectively.

Answer the following questions:

(1) What are the legitimate, total and illegitimate ranges for this RRNS?

(2) Is the given residue representation $(X_1, X_2, X_3, X_4) = (1, 2, 3, 3)$ error – free or not? Justify your answer.

(3) If the given residue representation $(X_1, X_2, X_3, X_4) = (1, 2, 3, 3)$ is not error-free, which residue digit is in error? What is the correct value of the residue-digit in error? What is the correct value of X?

Assumptions: (i). Overflow of the legitimate range cannot occur; (it is prevented).

(ii) At most one residue digit can be in error.

(iii) The hardware for converting the RNS into the weighted system is error-free.

(14) j

Answer:

(1). The ranges are:

Legitimate range = $[0 \quad (3\times4)-1] = [0 \quad 11]$.

Total range = $[0 \quad (3\times4\times5\times7)-1] = [0 \quad 419]$.

Illegitimate range = $[12 \quad 419]$.

(2). The residue representation $(X_1, X_2, X_3, X_4) = (1, 2, 3, 3)$ is <u>not</u> error-free; (an error has occured). This is due to the fact that $X = 178$ belongs to the illegitimate range.

(3). Since the projection belonging to the legitimate range is $X_3^* = 10$, (all the other projections belong to the illegitimate range), the residue digit $X_3 = 3$ is in error. The correct value of X_3 is $X_3 = \langle X_3^* \rangle_{m_3} = \langle 10 \rangle_5 = 0$, or $X_3 = 0$.

The correct value of X is $X = X_3^* = 10$.

References:

[1]. D. Mandelbaum, "Error correction in residue arithmetic", IEEE Transactions on Computers, vol C-21, pp. 538-545, June 1972.

[2]. M. H. Etzel and W. K. Jenkins, "Redundant residue number systems for error detection and correction in digital filters", IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. ASSP-28, pp. 538-544, October 1980.

[3]. F. Barsi and P. Maestrini, "Error correcting properties of redundant residue number systems", IEEE Transactions on Computers, vol. C-22, pp. 307-315, March 1973.

Appendix

In this appendix, the computations relating to example 1 (see pages 7–12 for example 1) are shown.

At first, using the moduli set $\{m_1, m_2, m_3, m_4, m_5\} = \{5, 6, 7, 11, 13\}$, the residue representation $(Z_1, Z_2, Z_3, Z_4, Z_5) = (2, 5, 5, 10, 2)$ is converted into its weighted form Z. Using the Chinese Remainder Theorem (CRT) one gets:

$$Z = \Big\langle \big\langle Z_1 \times (m_2 \times m_3 \times m_4 \times m_5)^{-1} \big\rangle_{m_1} \times m_2 \times m_3 \times m_4 \times m_5$$
$$+ \big\langle Z_2 \times (m_1 \times m_3 \times m_4 \times m_5)^{-1} \big\rangle_{m_2} \times m_1 \times m_3 \times m_4 \times m_5$$
$$+ \big\langle Z_3 \times (m_1 \times m_2 \times m_4 \times m_5)^{-1} \big\rangle_{m_3} \times m_1 \times m_2 \times m_4 \times m_5$$
$$+ \big\langle Z_4 \times (m_1 \times m_2 \times m_3 \times m_5)^{-1} \big\rangle_{m_4} \times m_1 \times m_2 \times m_3 \times m_5$$
$$+ \big\langle Z_5 \times (m_1 \times m_2 \times m_3 \times m_4)^{-1} \big\rangle_{m_5} \times m_1 \times m_2 \times m_3 \times m_4 \Big\rangle_{m_1 \times m_2 \times m_3 \times m_4 \times m_5}$$

$$= \Big\langle \langle 2 \times (6\times7\times11\times13)^{-1} \rangle_5 \times 6\times7\times11\times13 +$$

$$+ \langle 5 \times (5\times7\times11\times13)^{-1} \rangle_6 \times 5\times7\times11\times13 +$$

$$+ \langle 5 \times (5\times6\times11\times13)^{-1} \rangle_7 \times 5\times6\times11\times13 +$$

$$+ \langle 10 \times (5\times6\times7\times13)^{-1} \rangle_{11} \times 5\times6\times7\times13 +$$

$$+ \langle 2 \times (5\times6\times7\times11)^{-1} \rangle_{13} \times 5\times6\times7\times11 \Big\rangle_{5\times6\times7\times11\times13}$$

$$= \Big\langle \langle 2\times1 \rangle_5 \times 6006 + \langle 5\times1 \rangle_6 \times 5005 + \langle 5\times6 \rangle_7 \times 4290$$

$$+ \langle 10\times6 \rangle_{11} \times 2730 + \langle 2\times3 \rangle_{13} \times 2310 \Big\rangle_{30,030} =$$

$$= \Big\langle 2\times6006 + 5\times5005 + 2\times4290 + 5\times2730 + 6\times2310 \Big\rangle_{30030}$$

$$= \langle 73,127 \rangle_{30,030} = 13,067 \quad \text{or}$$

$$\boxed{Z = 13,067}.$$

Next, the m_i-projections of Z are computed; $(i = 1, 2, 3, 4, 5)$. The projections are denoted by $Z_1^*, \cdots, Z_5^*$ and the CRT is used to compute them.

- The projection Z_1^* is the result of converting $(Z_2, Z_3, Z_4, Z_5) = (5, 5, 10, 2)$ into its weighted form using set $\{m_2, m_3, m_4, m_5\} = \{6, 7, 11, 13\}$. Using the CRT one gets:

$$Z_1^* = \Big\langle \langle Z_2 \times (m_3 \times m_4 \times m_5)^{-1} \rangle_{m_2} \times m_3 \times m_4 \times m_5 + \langle Z_3 \times (m_2 \times m_4 \times m_5)^{-1} \rangle_{m_3} \times m_2 \times m_4 \times m_5 + \langle Z_4 \times (m_2 \times m_3 \times m_5)^{-1} \rangle_{m_4} \times m_2 \times m_3 \times m_5 + \langle Z_5 \times (m_2 \times m_3 \times m_4)^{-1} \rangle_{m_5} \times m_2 \times m_3 \times m_4 \Big\rangle_{m_2 \times m_3 \times m_4 \times m_5}.$$

Substituting in the above the given numerical values of $Z_2, Z_3, Z_4, Z_5, m_2, m_3, m_4, m_5$ one gets

$$Z_1^* = \Big\langle \langle 5 \times 5 \rangle_6 \times 1001 + \langle 5 \times 2 \rangle_7 \times 858 + \langle 10 \times 8 \rangle_{11} \times 546 + \langle 2 \times 2 \rangle_{13} \times 462 \Big\rangle_{6006} = 1,055$$

or $\boxed{Z_1^* = 1,055}$

- The projection Z_2^* is the result of converting $(Z_1, Z_3, Z_4, Z_5) = (2, 5, 10, 2)$ into its weighted form using set $\{m_1, m_3, m_4, m_5\} = \{5, 7, 11, 13\}$. Using the CRT one gets:

$$Z_2^* = \Big\langle \langle Z_1 \times (m_3 \times m_4 \times m_5)^{-1} \rangle_{m_1} \times m_3 \times m_4 \times m_5 + \langle Z_3 \times (m_1 \times m_4 \times m_5)^{-1} \rangle_{m_3} \times m_1 \times m_4 \times m_5 + \langle Z_4 \times (m_1 \times m_3 \times m_5)^{-1} \rangle_{m_4} \times m_1 \times m_3 \times m_5 + \langle Z_5 \times (m_1 \times m_3 \times m_4)^{-1} \rangle_{m_5} \times m_1 \times m_3 \times m_4 \Big\rangle_{m_1 \times m_3 \times m_4 \times m_5}$$

$$= 3,057 \text{ or } \boxed{Z_2^* = 3,057}$$

- The projection Z_3^* is the result of converting $(Z_1, Z_2, Z_4, Z_5) = (2, 5, 10, 2)$ into its weighted form using set $\{m_1, m_2, m_4, m_5\} = \{5, 6, 11, 13\}$. The CRT yields:

$$Z_3^* = \Big\langle \langle Z_1 \times (m_2 \times m_4 \times m_5)^{-1} \rangle_{m_1} \times m_2 \times m_4 \times m_5 + \langle Z_2 \times (m_1 \times m_4 \times m_5)^{-1} \rangle_{m_2} \times m_1 \times m_4 \times m_5 + \langle Z_4 \times (m_1 \times m_2 \times m_5)^{-1} \rangle_{m_4} \times m_1 \times m_2 \times m_5 + \langle Z_5 \times (m_1 \times m_2 \times m_4)^{-1} \rangle_{m_5} \times m_1 \times m_2 \times m_4 \Big\rangle_{m_1 \times m_2 \times m_4 \times m_5}$$

$$= 197 \text{ or } \boxed{Z_3^* = 197}.$$

- The projection Z_4^* is the result of converting $(Z_1, Z_2, Z_3, Z_5) = (2, 5, 5, 2)$ into its weighted form using set $\{m_1, m_2, m_3, m_5\} = \{5, 6, 7, 13\}$. The CRT yields:

$$Z_4^* = \Big\langle \langle Z_1 \times (m_2 \times m_3 \times m_5)^{-1} \rangle_{m_1} \times m_2 \times m_3 \times m_5 + \langle Z_2 \times (m_1 \times m_3 \times m_5)^{-1} \rangle_{m_2} \times m_1 \times m_3 \times m_5 + \langle Z_3 \times (m_1 \times m_2 \times m_5)^{-1} \rangle_{m_3} \times m_1 \times m_2 \times m_5 + \langle Z_5 \times (m_1 \times m_2 \times m_3)^{-1} \rangle_{m_5} \times m_1 \times m_2 \times m_3 \Big\rangle_{m_1 \times m_2 \times m_3 \times m_5}$$

$= 2147$ or $\boxed{Z_4^* = 2147}$.

- The projection Z_5^* is the result of converting $(Z_1, Z_2, Z_3, Z_4) = (2, 5, 5, 10)$ into its weighted form using set $\{m_1, m_2, m_3, m_4\} = \{5, 6, 7, 11\}$. The CRT gives:

$$Z_5^* = \Big\langle \langle Z_1 \times (m_2 \times m_3 \times m_4)^{-1} \rangle_{m_1} \times m_2 \times m_3 \times m_4 + \langle Z_2 \times (m_1 \times m_3 \times m_4)^{-1} \rangle_{m_2} \times m_1 \times m_3 \times m_4 + \langle Z_3 \times (m_1 \times m_2 \times m_4)^{-1} \rangle_{m_3} \times m_1 \times m_2 \times m_4 + \langle Z_4 \times (m_1 \times m_2 \times m_3)^{-1} \rangle_{m_4} \times m_1 \times m_2 \times m_3 \Big\rangle_{m_1 \times m_2 \times m_3 \times m_4}$$

$= 1517$ or $\boxed{Z_5^* = 1517}$